(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開平10－312321
(43)公開日　平成10年(1998)11月24日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	11/32		Ｇ０６Ｆ	11/32	Ｅ
	13/00	３５１		13/00	３５１Ｎ
	15/00	３２０		15/00	３２０Ｋ

審査請求　未請求　請求項の数３　ＯＬ　（全９頁）

(21)出願番号　特願平9－120484

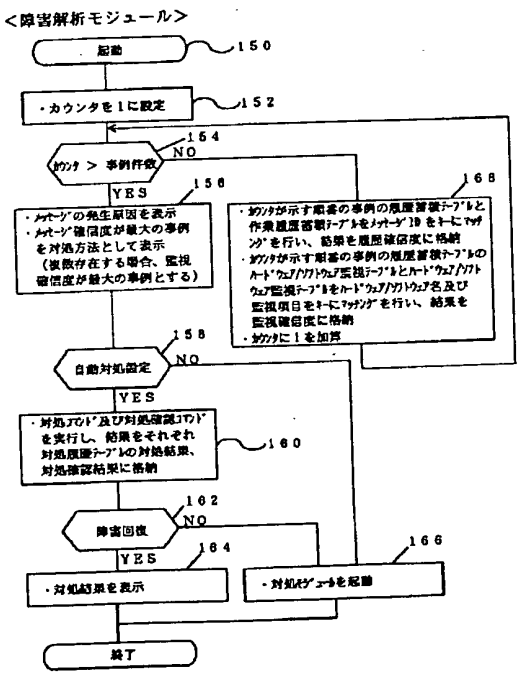
(22)出願日　平成９年(1997)５月12日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　小暮　慎一
東京都江東区新砂一丁目６番27号　株式会社日立製作所公共情報事業部内
(74)代理人　弁理士　小川　勝男

(54)【発明の名称】　オンラインシステム障害解析方法

(57)【要約】
【課題】本発明はオンラインシステムの障害の検出から対処方法の表示までの処理をリアルタイムに実現し、障害による影響を最小限に抑えることにある。
【解決手段】障害メッセージ発生時、カウンタを１にする（ステップ１５２）。メッセージテーブルの全事例についてカウンタの示す順番の事例の履歴確信度及び監視確信度を求める（ステップ１６８）。障害メッセージの発生原因の表示を行い、メッセージテーブルに格納されている履歴確信度が最大の事例を最適対処方法として表示する（履歴確信度が最大の履歴が複数存在する場合には監視確信度が最大の事例を表示する）（ステップ１５６）。対処が自動に設定されている場合、対処コマンド及び対処確認コマンドを実行し（ステップ１６０）。障害が回復した場合は対処結果を表示し（ステップ１６４）、回復しない場合は対処モジュールを起動し人による対処を行う（ステップ１６６）。

図３



【特許請求の範囲】

【請求項１】システムから出力されるデータに関係する情報を蓄積し、障害に関する情報と、システムから出力されるデータに関係する情報との対応関係を検査し、対応が一致したときは、障害に関係する原因と、障害の対処方法の表示を実現することを特徴とする障害解析方法。

【請求項２】請求項１において、ハードウェアの監視と、ソフトウェアの監視を常時行い、ハードウェア及びソフトウェアの障害について、障害に関する原因と、障害の対処方法の表示を実現することを特徴とする障害解析方法。

【請求項３】請求項２において、障害に関係する情報は、障害の原因に関係する情報と、過去の障害の事例に関係する情報を管理することを特徴とする障害解析方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はシステムから出力される情報からハードウェア及びソフトウェアの障害について、障害に関する原因と、障害の対処方法の表示を実現する障害解析方法に関し、特に障害の検出から対処までの処理に高速なリアルタイム性を要求されるオンラインシステムに関する。

【０００２】

【従来の技術】機器などのハードウェアの障害やアプリケーションプログラムなどのソフトウェアの障害に関し、障害の診断を行う装置やシステムが様々な分野で開発され、稼動している。これらのシステムの管理においては、障害解析が大きな役割を果たしている。例えば、特開平０６－１６１７６０号公報に示されているように機器の診断にリアルタイム性を持った装置を持ったものがある。この技術では、専門家によって行われていた診断を機械化することによって判定にばらつきがなく、迅速な診断を可能としている。また、特開平０８－２３７１８８号公報に示されているように通信端末装置は通信の履歴に関するデータを記憶し、通信障害時のデータをネットワークを介して情報蓄積装置に伝送することにより、通信端末装置の保守を効率良くできるようにしている。

【０００３】また、企業や官庁において、高速処理や信頼性が要求される分野で様々なオンラインシステムが稼動している。これらのシステムにおいては、機器などのハードウェア上でアプリケーションプログラムなどのソフトウェアが稼動しており、個々のハードウェアやソフトウェアの障害の診断を行っている。

【０００４】

【発明が解決しようとする課題】かかる従来の方法においては、次のような問題がある。

【０００５】すなわち、ハードウェアとソフトウェアの障害が同時に複数件数発生した場合、障害の検出から障害の対処までの処理を高速に実現することは困難な作業となる。

【０００６】このように従来の方法は、ハードウェアまたはソフトウェアの個々の障害に対応するもので、複数のハードウェア装置及びソフトウェアから構成され相互に影響を与える可能性のあるシステムの障害には対処できないという問題があった。

【０００７】本発明の目的は、複数のハードウェア装置及びソフトウェアから構成されるオンラインシステムの障害にリアルタイムに対処可能なオンラインシステム障害解析方法を提供することにある。

【０００８】本発明の他の目的は、従来人間が行っていた複雑な障害回復作業を機械化することにより作業の精度及び速度の向上や作業の容易性を実現し、障害による損害を最小限に抑えて、専門の知識を持たない人でも障害回復作業を行うための手段を提供することにある。

【０００９】

【課題を解決するための手段】本発明は、オンラインシステムから監視端末に出力されるメッセージの履歴に関係する情報の一定期間の蓄積とハードウェア／ソフトウェアの稼動状況の監視を行い、障害が発生した際に、障害の原因の表示と過去の最適事例の対処方法の表示を行う。

【００１０】オンラインシステムから監視端末に出力されるメッセージをメッセージ監視モジュールにおいて常時監視し、出力メッセージの一定時間の履歴を随時、履歴蓄積テーブルに蓄積しておく。障害が発生した際には、障害発生時点の履歴蓄積テーブルを作業履歴蓄積テーブルとしてコピーする。この作業履歴蓄積テーブルとメッセージテーブルの過去の事例の履歴をメッセージＩＤをキーにマッチングを行い、一致した数を履歴確信度として格納する。続いて、障害が発生した時点のハードウェア／ソフトウェアの稼動状況とメッセージテーブルの過去の事例が発生した時点のハードウェア／ソフトウェアの稼動状況をハードウェア／ソフトウェア名及び監視項目をキーにマッチングを行い、一致した数を監視確信度として格納する。そして、履歴確信度が最大の事例を最適事例とする（履歴確信度が最大の事例が複数存在する際には、監視確信度が最大の事例とする）。なお、障害メッセージの原因及び分類情報、過去の事例情報はメッセージテーブルで管理する。続いて、障害の原因の表示と最適事例の対処方法の表示を行う。対処による障害回復については、対処コマンドと対処確認コマンドの実行及び結果確認により行う。

【００１１】ハードウェアの監視と、ソフトウェアの監視を常時行い、ハードウェア及びソフトウェアの障害について、障害に関する原因と、障害の対処方法の表示をリアルタイムに実現することを特徴とする障害解析方法。

【００１２】障害に関係する情報は、障害の原因に関係する情報と、過去の障害の事例に関係する情報の２種類とする。

【００１３】

【発明の実施の形態】以下、本発明の実施の形態を詳細に説明する。

【００１４】図１、図２、図３、図４は、本発明をオンラインシステムに適用した場合の処理手順の実施の形態を示すフローチャートであり、図５は、本発明に係るオンラインシステム障害解析方法の構成を示すブロック図である。図６及び図７は、本発明に係るオンラインシステム障害解析方法を実現する際に利用するデータテーブルである。

【００１５】図５において、障害解析処理を監視端末における５つのモジュールにより実現する。メッセージ監視モジュール１２は、まず、オンラインシステム１０からメッセージ取得部１１を通じて監視端末側へ出力される全てのメッセージを履歴蓄積テーブル１７へ格納する。次に、出力メッセージに関する分類情報をメッセージテーブル１９へ参照し、履歴蓄積テーブル１７へ格納する。ハードウェア監視モジュール１３は、ハードウェア稼動状況を常時監視しており、ハードウェア監視テーブル２０に格納する。ソフトウェア監視モジュール１４は、ソフトウェア稼動状況を常時監視しており、ソフトウェア監視テーブル２１に格納する。履歴蓄積テーブル１７は、オンラインシステム１０から出力されるメッセージの履歴に関係する情報を蓄積する為に用いられる。作業履歴蓄積テーブル１８は、障害発生時点のメッセージの履歴に確保し、メッセージテーブルの過去の事例の履歴との比較を行う為に用いられる。対処履歴テーブル２２は、障害発生後の対処結果を格納する為に用いられる。メッセージテーブル１９には、監視対象のメッセージがメッセージＩＤをキーとして、ハードウェア／ソフトウェア別、システムメッセージ／アプリケーションメッセージ別に分類した形で格納されている。ハードウェア監視テーブル２０は、ハードウェアの稼動状況を常時監視する為のテーブルであり、監視対象の設定は予め設定しておくものとする。ソフトウェア監視テーブル２１は、ソフトウェアの稼動状況を常時監視する為のテーブルであり、監視対象の設定は予め設定しておくものとする。障害解析モジュール１５は、障害が発生した際に起動され、障害の原因の表示と過去の最適事例の対処方法の表示を行い、対処結果を対処履歴テーブル２２に格納する。対処履歴テーブル２２は、発生した障害メッセージに対する対処の情報を格納する為のテーブルである。

【００１６】図６及び図７は、図５における各テーブルのレコードフォーマットであり、以下、図６及び図７の各テーブルの関係について説明する。図６Ａ＜履歴蓄積テーブル及び作業履歴蓄積テーブル＞は、図５の履歴蓄積テーブル１７及び作業履歴蓄積テーブル１８のレコードフォーマットである。ここで、図６Ａ＜履歴蓄積テーブル及び作業履歴蓄積テーブル＞の各項目について説明する。メッセージＩＤは図５のオンラインシステム１０から図５の監視端末に出力されるメッセージを識別するキーとして用い、メッセージが発生する度に図５Ａ＜履歴蓄積テーブル＞に蓄積される。発生時刻にはメッセージが出力された時刻を格納する。ソフト／ハード区分及び障害／警告区分には図６Ｂ＜メッセージテーブル＞を参照し、格納する。メッセージには出力されたメッセージの中のコメント情報をテキスト形式で格納する。図６Ｂ＜メッセージテーブル＞は、図５のメッセージテーブル１９のレコードフォーマットである。続いて、図６Ｂ＜メッセージテーブル＞の各項目について説明する。メッセージＩＤは図６Ｂ＜メッセージテーブル＞におけるキーとして管理されており、ハードウェア／ソフトウェア別、システムメッセージ／アプリケーションメッセージ別に分類されている。障害／警告区分はメッセージが障害を意味するか警告を意味するかを示すものである。原因はマニュアルに掲載されている情報であり、重要度はメッセージの持つ意味合いを示すものである。事例件数は、過去の事例を図６Ｂ＜メッセージテーブル＞に何件格納してあるかを示す。障害メッセージについてのみ、過去の事例が発生した時の出力メッセージの履歴を履歴蓄積テーブルで、過去の事例の対処に関する情報を対処テーブルでそれぞれ管理している。続いて、図６Ｃ＜対処テーブル＞の各項目について説明する。図６Ｃ＜対処テーブル＞には発生した障害に対して行った対処方法を格納する。対処策には実際の対処策の内容を格納する。対処コマンドには実際の対処に用いたコマンドを格納し、対処結果コマンドには対処コマンドの実行結果を格納する。対処確認コマンドには対処コマンドが正しく実行されたかを確認するコマンドを格納し、対処確認結果には対処確認コマンドの実行結果の確認事項を格納する。履歴確信度には障害発生時点の図６Ａ＜作業履歴蓄積テーブル＞と図６Ｂ＜メッセージテーブル＞に格納されている事例の履歴蓄積テーブルとのメッセージＩＤをキーとしたマッチングの結果を格納する。監視確信度には障害発生時点のハードウェア／ソフトウェア稼動状況をハードウェア／ソフトウェア名及び監視項目をキーとしたマッチングの結果を格納する。自動／手動対処設定には、過去の障害の中で最も確信度が高かった場合に自動的に対処を行うかどうかを設定する。続いて、図７Ｄ＜ハードウェア監視テーブル＞は、図５のハードウェア監視テーブル２０のレコードフォーマットであり、ハードウェア別に監視項目及び監視結果を設定する。図７Ｅ＜ソフトウェア監視テーブル＞は、図５のソフトウェア監視テーブル２１のレコードフォーマットであり、ソフトウェア別に監視項目及び監視結果を設定する。図７Ｆ＜対処履歴テーブル＞は、図５の対処履歴テーブル２２のレコードフォーマットであり、発生した障害メッセー

ジに対する対処が終了した時点で格納する為のテーブルであり、障害解析が終了した時点で図４のメッセージテーブル１９に事例として格納する。

【００１７】次に図１、図２、図３、図４のフローチャートに基いて図５の各動作を説明する。

【００１８】図５のメッセージ監視モジュール１２の起動（ステップ１００）から終了までの動作を説明する。障害解析を終了するまで処理を行う（ステップ１０２）。まず、図５のオンラインシステム１０よりメッセージが出力されているかを確認する（ステップ１０４）。出力されていればメッセージＩＤをキーに図５のメッセージテーブル１９を参照し、図５の履歴蓄積テーブル１７に出力メッセージに関する情報を蓄積する（ステップ１０６）。蓄積する際、図５メッセージテーブル１９からメッセージＩＤ、発生時刻、ソフト／ハード区分、障害／警告区分、メッセージを参照する。図５のメッセージテーブル１９に登録されていないメッセージが出力された場合には履歴蓄積テーブルへの蓄積を行わない。次に、出力メッセージが障害メッセージであるかを判別し（ステップ１０８）、障害である場合以下の処理を行う。まず、障害メッセージ発生時点の履歴蓄積テーブルを作業履歴蓄積テーブルとしてコピーする（ステップ１１０）。続いて、障害メッセージがハードウェアに関するものであれば（ステップ１１２）、ハードウェア監視テーブルを更新する（ステップ１１４）。ハードウェアに関するものでなければソフトウェア監視テーブルを更新する（ステップ１１６）。続いて、図５のメッセージテーブル１９に対処方法が存在する場合には（ステップ１１８）、図５の障害解析モジュールを起動する（ステップ１２０）。対処方法が存在しない場合には、障害の原因のみを表示する（ステップ１２２）。対処方法が存在するかの判別は図６Ｂ＜メッセージテーブル＞の事例件数が０がどうかで行う。

【００１９】続いて図５のハードウェア監視モジュール１３の起動（ステップ１３０）から終了までの処理を説明する。ハードウェア監視モジュール１３では、障害解析が終わるまで（ステップ１３２）、ハードウェア管理テーブル２０にハードウェアの稼動状況を格納する（ステップ１３４）。

【００２０】続いて図５のソフトウェア監視モジュール１４の起動（ステップ１４０）から終了までの処理を説明する。ソフトウェア監視モジュール１４では、障害解析が終わるまで（ステップ１４２）、ソフトウェア管理テーブル２１にソフトウェアの稼動状況を格納する（ステップ１４４）。

【００２１】続いて図５の障害解析モジュール１５の起動（ステップ１５０）から終了までの処理を説明する。まず、過去の事例の中から最適事例を求める際に用いるカウンタを１にする（ステップ１５２）。まず、カウンタが図６Ｂ＜メッセージテーブル＞の事例件数より大きいかを判別する（ステップ１５４）。大きくない場合、カウンタの示す順番に格納されている事例の履歴蓄積テーブルと作業履歴蓄積テーブルとのメッセージＩＤをキーとしたマッチング結果の図６Ｃ＜対処テーブル＞の履歴確信度へ格納する。続いて、カウンタの示す順番に格納されている事例の図６Ａ＜履歴蓄積テーブル＞のソフトウェア／ハードウェア監視テーブルと図７Ｄ及びＥのソフトウェア／ハードウェア監視テーブルとのハードウェア／ソフトウェア名及び監視項目をキーとしたマッチングの結果を監視確信度へ格納する。続いて、カウンタに１を加える（ステップ１６８）。カウンタが図６Ｂ＜メッセージテーブル＞の事例件数より大きい場合、以下の処理を行う（ステップ１５４）。履歴確信度が最大の事例を最適事例とし（履歴確信度が最大の事例が複数存在する際には、監視確信度が最大の事例とする）、障害の原因の表示と過去の最適事例表示を行う（ステップ１５６）。続いて、図６Ｃ＜対処テーブル＞の自動／手動対処設定を参照し、対処が自動設定になっているかを判別する（ステップ１５８）。自動設定になっていない場合、対処モジュールを起動し、人による対処を行う（ステップ１６６）。自動設定になっている場合、図６Ｃ＜対処テーブル＞の対処コマンド及び対処確認コマンドを実行する（ステップ１６０）。続いて、障害回復したどうかを図７Ｆ＜対処履歴テーブル＞の対処結果と対処確認結果を比較して判別し（ステップ１６２）、回復した場合には障害回復の表示を行う（ステップ１６４）。回復していない場合、対処モジュールを起動し、人による対処を行う（ステップ１６６）。

【００２２】続いて図５の対処モジュール１６の起動（ステップ１７０）から終了までの処理を説明する。まず、人による対処入力を待ち（ステップ１７２）、入力後、図７Ｆ＜対処履歴テーブル＞に対処結果及び対処確認結果を格納する（ステップ１７４）。障害回復したどうかを図７Ｆ＜対処履歴テーブル＞の対処結果と対処確認結果を比較して判別し（ステップ１７６）、回復した場合には障害回復の表示を行う（ステップ１７８）。回復していない場合、人による対処を行う（ステップ１７２、１７４、１７６）。

【００２３】

【発明の効果】以上述べたように、本発明によれば、複数のハードウェア装置及びソフトウェアから構成されるオンラインシステムの障害にリアルタイムな対処を可能とすることができるので、障害発生による損害を最小限に抑えることが出来る。また、従来人間が行っていた複雑な障害回復作業を機械化して支援することにより、専門の知識を持たない人でも障害回復作業を行うことができる。

【図面の簡単な説明】

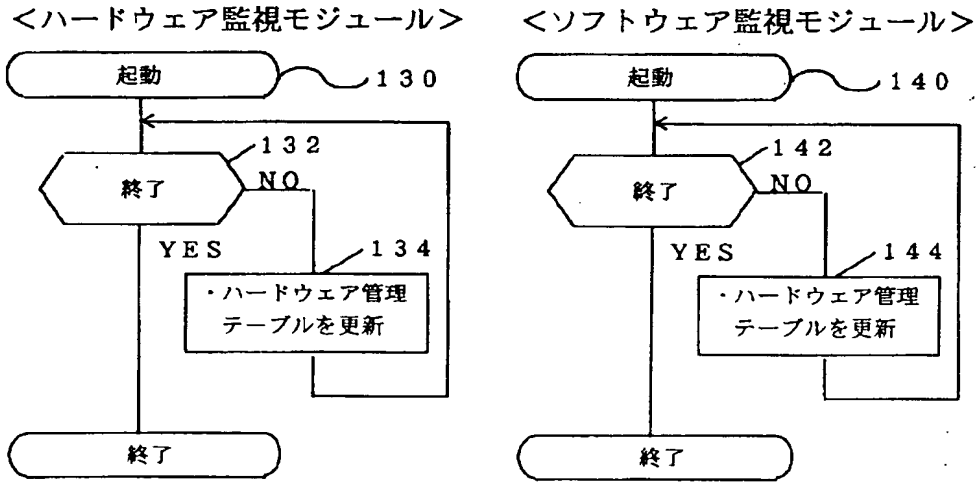
【図１】本発明の処理手順の実施の形態を示すフローチャートである。

【図２】本発明の処理手順の実施の形態を示すフローチャートである。
【図３】本発明の処理手順の実施の形態を示すフローチャートである。
【図４】本発明の処理手順の実施の形態を示すフローチャートである。
【図５】本発明に係わるオンラインシステム障害解析方法を構成するシステムブロック図である。
【図６】本発明に係わるオンラインシステム障害解析システムを構成するデータテーブルである。
【図７】本発明に係わるオンラインシステム障害解析システムを構成するデータテーブルである。
【符号の説明】

１０　オンラインシステム
１１　メッセージ取得部
１２　メッセージ監視モジュール
１３　ハードウェア監視モジュール
１４　ソフトウェア監視モジュール
１５　障害解析監視モジュール
１６　対処モジュール
１７　履歴蓄積テーブル
１８　作業履歴蓄積テーブル
１９　メッセージテーブル
２０　ハードウェア監視テーブル
２１　ソフトウェア監視テーブル
２２　対処履歴監視テーブル。

【図２】

図２



【図７】

図７

D　<ハードウェア監視テーブル>

項番	ハードウェア名	監視項目	結果
1	H1	電源	ON
2	H2	監視	OFF
		電源	ON
:	:	:	:

E　<ソフトウェア監視テーブル>

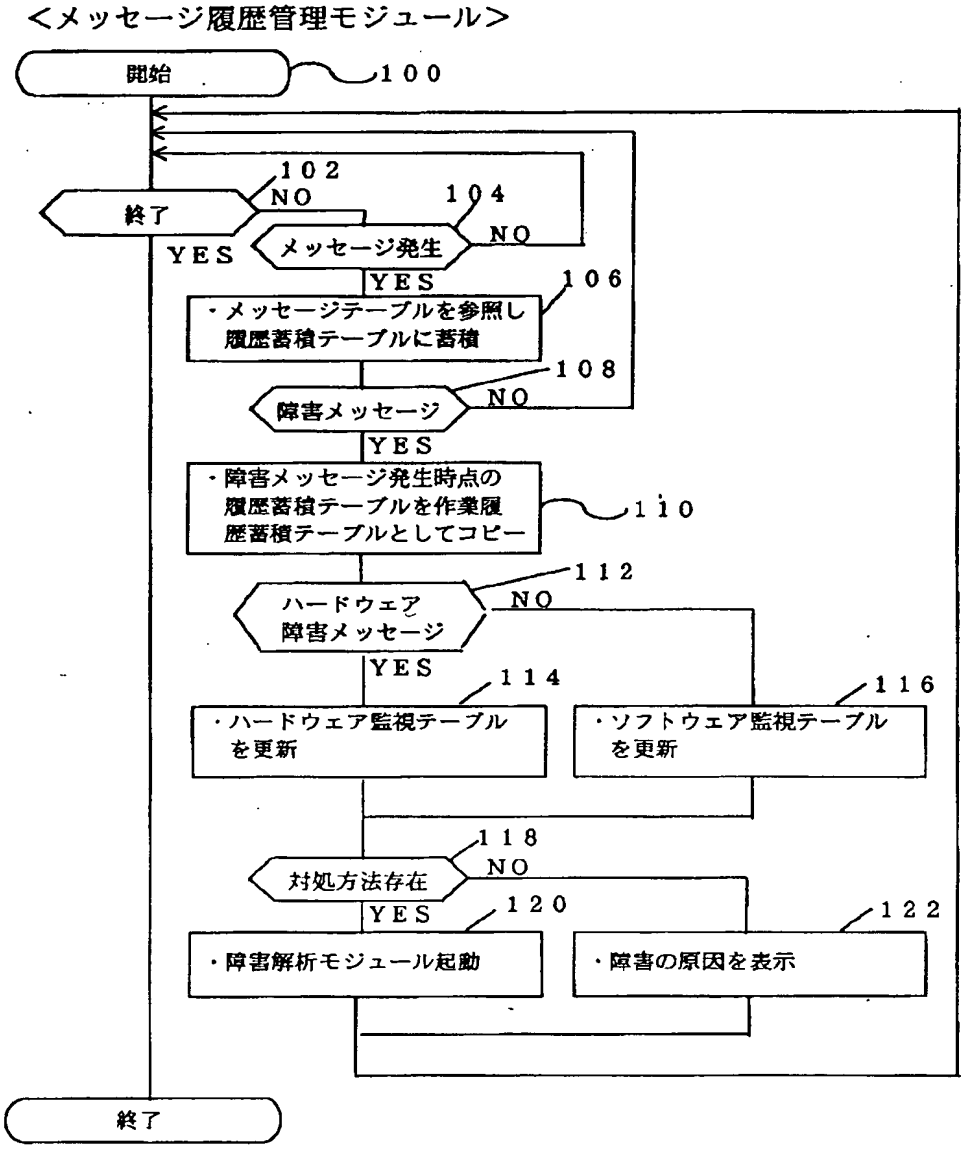
項番	ソフトウェア名	監視項目	結果
1	S1	起動	ON
2	S2	起動	ON
:	:	:	:

F　<対処履歴テーブル>

メッセージID	対処テーブル
HSW002	
SAV001	
:	:

【図１】

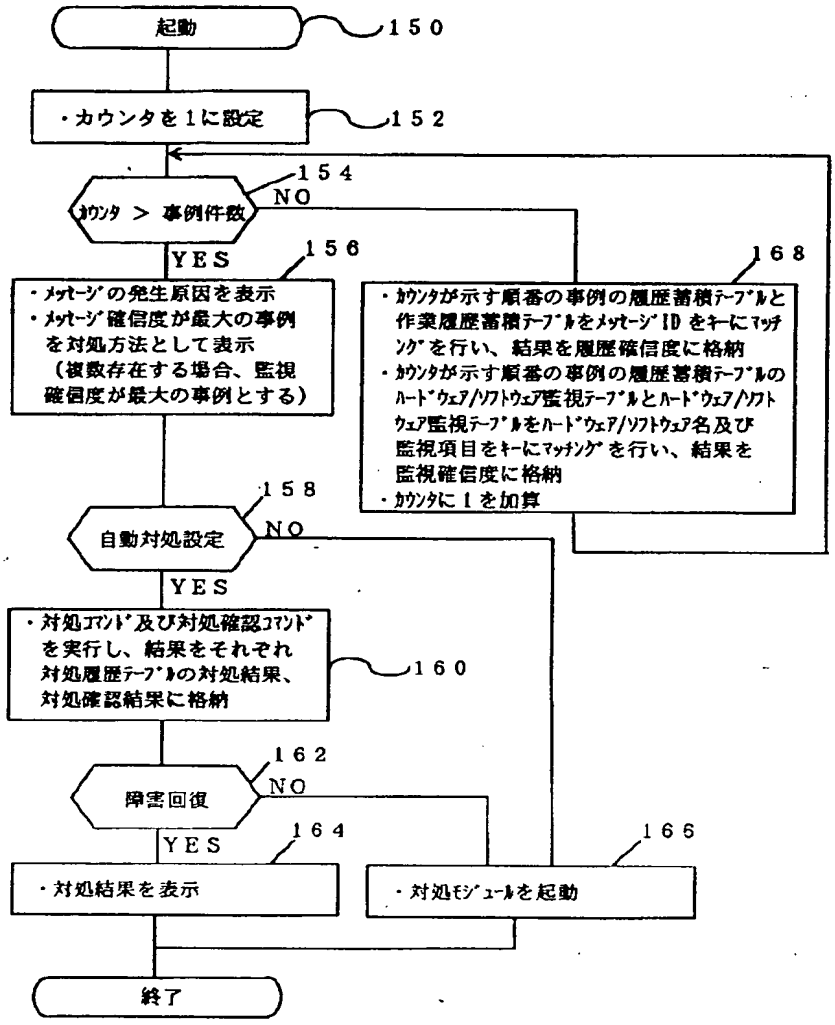
図１


<メッセージ履歴管理モジュール>
開始
100
102
NO
終了
YES
104
NO
メッセージ発生
YES
106
・メッセージテーブルを参照し履歴蓄積テーブルに蓄積
108
NO
障害メッセージ
YES
・障害メッセージ発生時点の履歴蓄積テーブルを作業履歴蓄積テーブルとしてコピー
110
112
NO
ハードウェア障害メッセージ
YES
114
・ハードウェア監視テーブルを更新
116
・ソフトウェア監視テーブルを更新
118
NO
対処方法存在
YES
120
・障害解析モジュール起動
122
・障害の原因を表示
終了

【図３】

図３

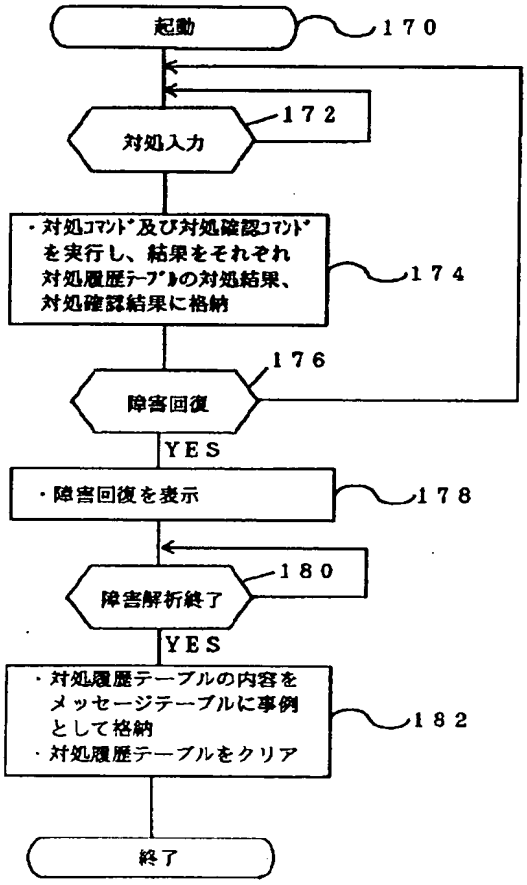
<障害解析モジュール>



【図４】

図４

<対処モジュール>



【図６】

図６

A　<履歴蓄積テーブル、作業履歴蓄積テーブル>

項番	メッセージID	発生時刻	ソフト/ハード区分 ※1	障害/警告区分 ※2	メッセージ
1	HSW001	10:40:00	2	1	AAAAAAAAAA
2	HSW002	10:40:10	2	1	BBBBBBBBBB
3	SAW001	10:40:15	1	1	PPPPPPPP
4	SSW001	10:40:30	1	1	VVVVVVVVV
5	HSE001	10:40:40	2	2	WWWWW
:	:	:	:	:	:

※1…ソフト:1、ハード:2　　※2…警告:1、障害:2

B　<メッセージテーブル>

ハード/ソフト区分 ※1	メッセージ区分 ※2	項番	メッセージID	障害/警告区分 ※3	原因	重要度	事例件数	事例	
								事例1	…
								履歴蓄積テーブル1	対処テーブル1
1	1	1	HSW001	1	電源	4	0		
		2	HSW002	1	電源	4	3		
		:	:	:	:	:	:		
	2	1	HAW001	1	アクセス不能	4	0		
		2	HPE001	2	アクセス不能	8	3		
		:	:	:	:	:	:		
2	1	1	SSW001	1	起動不能	4	0		
		2	SSE001	2	起動不能	12	2		
		:	:	:	:	:	:		
	2	1	SAW001	1	設定ミス	4	0		
		2	SAE001	2	設定ミス	8	2		
		:	:	:	:	:	:		

※1…ハードウェア:1、ソフトウェア:2 ※2…システムメッセージ:1、アプリケーションメッセージ:2 ※3…警告:1、障害:2

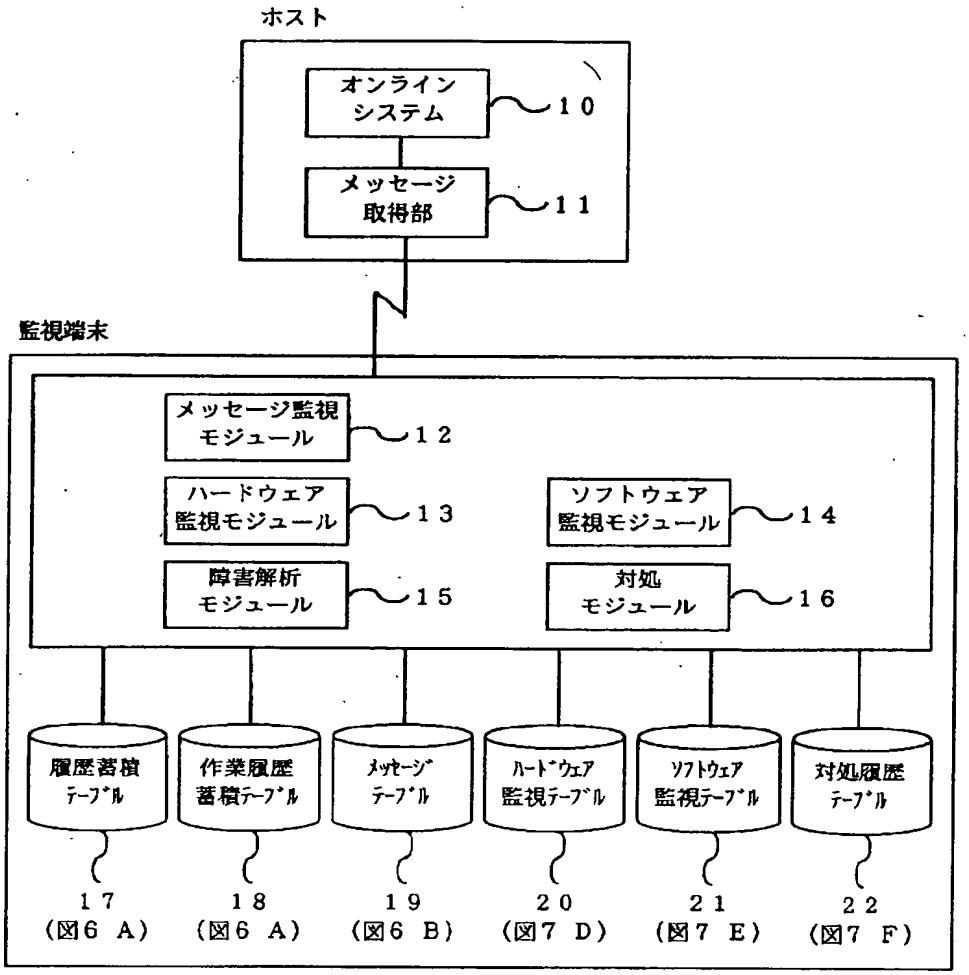
C　<対処テーブル>

対処策	対処コマンド	対処結果	対処確認コマンド	対処確認結果	履歴確信度	登録確信度	自動/手動設定 ※1
AAA	BBB	CCC	DDD	CCC	4	3	2

※1…自動:1、手動:2

【図５】

図５


ホスト
オンライン
システム
１０
メッセージ
取得部
１１
監視端末
メッセージ監視
モジュール
１２
ハードウェア
監視モジュール
１３
ソフトウェア
監視モジュール
１４
障害解析
モジュール
１５
対処
モジュール
１６
履歴蓄積
ﾃｰﾌﾞﾙ
作業履歴
蓄積ﾃｰﾌﾞﾙ
ﾒｯｾｰｼﾞ
ﾃｰﾌﾞﾙ
ﾊｰﾄﾞｳｪｱ
監視ﾃｰﾌﾞﾙ
ｿﾌﾄｳｪｱ
監視ﾃｰﾌﾞﾙ
対処履歴
ﾃｰﾌﾞﾙ
１７
（図６ Ａ）
１８
（図６ Ａ）
１９
（図６ Ｂ）
２０
（図７ Ｄ）
２１
（図７ Ｅ）
２２
（図７ Ｆ）